

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-72721

(P2004-72721A)

(43) 公開日 平成16年3月4日(2004.3.4)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04L 9/32	H04L 9/00	5 J 104
G09C 1/00	G09C 1/00	
H04L 9/08	H04L 9/00	

審査請求 未請求 請求項の数 15 O L (全 28 頁)

(21) 出願番号	特願2003-151473 (P2003-151473)	(71) 出願人	000005821
(22) 出願日	平成15年5月28日 (2003.5.28)		松下電器産業株式会社
(31) 優先権主張番号	特願2002-170251 (P2002-170251)		大阪府門真市大字門真1006番地
(32) 優先日	平成14年6月11日 (2002.6.11)	(74) 代理人	100090446
(33) 優先権主張国	日本国 (JP)		弁理士 中島 司朗
		(72) 発明者	松崎 なつめ
			大阪府門真市大字門真1006番地 松下
			電器産業株式会社内
		(72) 発明者	館林 誠
			大阪府門真市大字門真1006番地 松下
			電器産業株式会社内
		(72) 発明者	横田 薫
			大阪府門真市大字門真1006番地 松下
			電器産業株式会社内

最終頁に続く

(54) 【発明の名称】 認証システム、鍵登録装置及び方法

(57) 【要約】

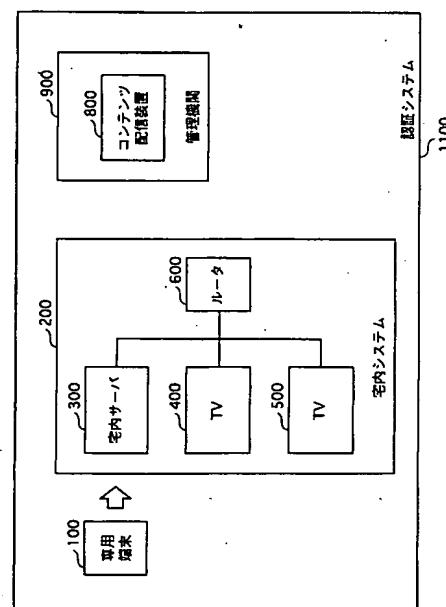
【課題】コンテンツをユーザ宅内での個人使用に限定するために、ユーザ宅内の機器を簡易に設定することが可能な、認証システム及び鍵登録装置を提供することを目的とする。

【解決手段】第1機器と第2機器との間において、認証を行う認証システムである。前記第2機器は、当該第2機器に固有の識別子から、所定の鍵生成アルゴリズムに基づいて生成された第2鍵情報を記憶している。鍵登録装置は、前記識別子の入力を受け付け、前記鍵生成アルゴリズムに基づいて第1鍵データを生成し、前記第1機器に送信する。前記第1機器は、前記第1鍵データを受信して記憶する。

前記第1機器は、前記第2機器と通信する際、前記第1鍵データを用いて認証し、前記第2機器は、第2鍵データを用いて認証を受ける。

この構成により、鍵データを登録された機器以外と通信することを防ぐ。また、外部への接続手段を持たない機器でも実現できる。

【選択図】 図1



【特許請求の範囲】

【請求項1】

第1機器と第2機器との間において、認証を行う認証システムであって、
前記第2機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第1鍵データを生成し、生成した第1鍵データを前記第1機器に送信する鍵登録装置と、
前記鍵登録装置から前記第1鍵データを受信して記憶し、当該第1鍵データを用いて前記第2機器を認証する第1機器と、
前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第2鍵データを予め記憶しており、前記第2鍵データを用いて前記第1機器による認証を受ける第2機器と
から構成されることを特徴とする認証システム。 10

【請求項2】

第1機器と第2機器との間において、認証を行う認証システムであって、
前記第2機器に固有の機器識別子の入力を受け付け、鍵生成アルゴリズムに基づいて前記機器識別子から第1鍵データを生成し、生成した第1鍵データを前記第1機器に送信する鍵登録装置と、
前記鍵登録装置から受信する前記第1鍵データを記憶し、前記第1鍵データを用いて前記第2機器を認証する第1機器と、
前記機器識別子からそれぞれ異なる鍵生成アルゴリズムに従って生成される複数の鍵データを予め記憶しており、前記複数の鍵データの内、前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第2鍵データを選択し、選択した第2鍵データを用いて、前記第1機器による認証を受ける第2機器と
から構成されることを特徴とする認証システム。 20

【請求項3】

前記第1機器は、更に、鍵登録装置の無効化を管理する管理機関により生成され、前記鍵登録装置の無効化を示す鍵無効化情報を受け取り、前記鍵登録装置から受信した第1鍵データを無効化し、
前記第2機器は、前記鍵無効化情報を受け取り、前記第2鍵データを無効化すること
を特徴とする請求項2記載の認証システム。 30

【請求項4】

前記認証システムは、更に、鍵再登録装置を含み、
前記鍵再登録装置は、前記第2機器に固有の機器識別子の入力を受け付け、前記鍵登録装置の鍵生成アルゴリズムと異なる鍵生成アルゴリズムに基づいて前記第2機器に固有な機器識別子から第3鍵データを生成し、生成した第3鍵データと前記機器識別子とを前記第1機器に送信し、
前記第1機器は、更に、前記鍵再登録装置から受信する前記第3鍵データ及び前記機器識別子を対応付けて記憶し、前記第3鍵データを用いて前記第2機器を認証し、
前記第2機器は、更に、前記複数の鍵データの内、前記第3鍵データを生成した鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第4鍵データを用いて、前記第1機器による認証を受ける
ことを特徴とする請求項3記載の認証システム。 40

【請求項5】

前記第1機器は、前記管理機関により生成され、無効化された鍵登録装置に固有の識別子を更に含む鍵無効化情報を受け取り、更に受け取った識別子を無効化識別子として記憶し、
鍵登録装置から、第1鍵データと共に、前記鍵登録装置に固有の識別子を受け取り、受け取った識別子が前記無効化識別子と一致するか否かを判断し、一致する場合、前記鍵登録装置から前記第1鍵データを受け取ることを拒否する
ことを特徴とする請求項3記載の認証システム。 50

【請求項 6】

前記第 1 機器は、前記管理機関により生成され、前記鍵無効化情報に前記管理機関の署名を施して生成された署名データを更に含む前記鍵無効化情報を受け取り、
前記署名データを検証し、検証結果が成功であれば、前記識別子を無効化識別子として記憶すること
を特徴とする請求項 5 記載の認証システム。

【請求項 7】

第 2 機器が有する、第 1 機器と前記第 2 機器との間で認証を行うための第 2 鍵データと同一の第 1 鍵データを、前記第 1 機器に設定する鍵登録装置であって、
前記第 2 機器に固有の識別子の入力を受け付ける入力手段と、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第 1 鍵データを生成する鍵データ生成手段と、
生成した前記第 1 鍵データを前記第 1 機器へ出力する出力手段と
から構成されることを特徴とする鍵登録装置。

10

【請求項 8】

前記出力手段は、前記第 1 鍵データを暗号化して前記第 1 機器へ出力し、
前記第 1 機器は、暗号化された第 1 鍵データを受け取り、復号すること
を特徴とする請求項 7 記載の鍵登録装置。

【請求項 9】

前記出力手段は、前記第 1 鍵データを、ネットワークを介して前記第 1 機器へ送信し、
前記第 1 機器は、ネットワークを介して前記第 1 鍵データを受信すること
を特徴とする請求項 7 記載の鍵登録装置。

20

【請求項 10】

前記鍵登録装置は、
前記第 1 機器を認証する認証手段を含み、
前記鍵データ生成手段は、前記認証手段による認証結果が成功の場合、前記第 1 鍵データを生成すること
を特徴とする請求項 7 記載の鍵登録装置。

【請求項 11】

前記鍵データ生成手段は、前記識別子から前記第 1 鍵データを生成する関数を記憶しており、
前記鍵データ生成手段は、前記関数を読み出し、読み出した関数に前記識別子を代入して前記第 1 鍵データを生成すること
を特徴とする請求項 7 記載の鍵登録装置。

30

【請求項 12】

前記鍵登録装置は、ICカードであり、携帯電話又は情報携帯端末に接続可能であり、
前記出力手段は、前記携帯電話又は前記情報携帯端末を介して前記第 1 機器へ出力すること
を特徴とする請求項 7 記載の鍵登録装置。

【請求項 13】

第 2 機器が有する、第 1 機器と前記第 2 機器との間で認証を行うための第 2 鍵データと同一の第 1 鍵データを、前記第 1 機器に設定する鍵登録装置で用いられるプログラムであって、
前記第 2 機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第 1 鍵データを生成する鍵データ生成ステップと、
生成した前記第 1 鍵データを前記第 1 機器へ出力する出力ステップと
を含むことを特徴とするプログラム。

40

【請求項 14】

第 2 機器が有する、第 1 機器と前記第 2 機器との間で認証を行うための第 2 鍵データと同一の第 1 鍵データを、前記第 1 機器に設定する鍵登録装置で用いられる方法であって、

50

前記第2機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第1鍵データを生成する鍵データ生成ステップと、
生成した前記第1鍵データを前記第1機器へ出力する出力ステップと
を含むことを特徴とする方法。

【請求項15】

第2機器が有する、第1機器と前記第2機器との間で認証を行うための第2鍵データと同一の第1鍵データを、前記第1機器に設定する鍵登録装置で用いられるプログラムを記憶している、コンピュータ読み取り可能な記録媒体であって、前記プログラムは、
前記第2機器に固有の識別子の入力を受け付ける入力ステップと、
鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第1鍵データを生成する鍵データ生成ステップと、
生成した前記第1鍵データを前記第1機器へ出力する出力ステップと
を含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数の機器間において暗号認証通信を行うシステムに関する。

【0002】

【従来の技術】

近年、パッケージメディアやインターネット、放送を用いた様々な音楽、映像コンテンツ配信サービスが広がっている。こういったサービスに対応して、コンテンツの著作権保護者の意思を反映したコンテンツ保護技術が必要になる。コンテンツ著作権保護者の意思としては、(1)コンテンツ配信サービスを有料とし、コンテンツの配信契約を結んだユーザの宅内での個人使用に限定したい、(2)不特定多数者がアクセスできるインターネットへの送信は許可しない、などがある。

【0003】

このような、コンテンツの著作権保護者の意思を実現するためのコンテンツ保護技術の1つに、DTCP(Digital Transmission Content Protection)と呼ばれる規格がある。DTCPは、高速シリアルバス規格の1つのIEEE1394により規定されるバスを介して配信されるデジタルコンテンツの保護規格である。DTCPについては、非特許文献1に詳しい。

【0004】

DTCPでは、DTLA(Digital Transmission Licensing Administrator, LLC)と呼ばれる管理者の管理下でDTCP規格に準拠した機器を相互接続し、その間で暗号認証通信を行っている。その仕組みを以下に示す。

(1)送信機器及び受信機器は、DTLAから配布された秘密鍵を備えている。この秘密鍵の配布はDTLAとの契約に基づいて機器に配布される。なお、この秘密鍵の配布を受けた機器は、秘密鍵の管理実装方法を規定される。また、コンテンツのインターネットへの送信はDTCPの契約で禁止されている。

【0005】

(2)送信機器と受信機器とは、上記秘密鍵を用いて相互認証を行う。また、送信機器は、保護が必要となるコンテンツを、認証により共有した鍵で暗号化して送信する。

(3)送信機器は、最大63台までの受信機器にコンテンツを復号するための鍵を与える。IEEE1394のAVCコマンドの制限及び台数制限により、コンテンツの個人使用限定を容易に実現する。

【0006】

次に、Kerberos(ケルベロス)を利用した認証システムの概略を説明する。Kerberosについては、非特許文献2に詳しい。

10

20

30

40

50

Kerberosでは、正規の機器は予めKerberosサーバに登録されているとする。一例としてコンテンツの利用を受ける際、機器はまず、Kerberosサーバにアクセスし、登録している情報を元に1回目の認証を受けて、Kerberosサーバによりその日有効なチケット（イニシャルチケット）を獲得する。次に、機器は、当該サービスを提供するサーバにアクセスし、先にKerberosサーバからもらったイニシャルチケットを提示して、2回目の認証を受け、コンテンツを利用する。

【0007】

このように、Kerberosでは、認証を2回に分けて行うことにより、登録されている機器は、決められている有効期限内であればどのサービスも自由に利用することが出来る。

【0008】

【非特許文献1】

「5C Digital Transmission Content Protection White Paper」Revision 1.0 July 14, 1998

【0009】

【非特許文献2】

ブライアン・タン著、桑村通訳「KERBEROS ネットワーク認証システム」ピアソン出版、1999

【0010】

【発明が解決しようとする課題】

しかしながら、上記何れの方法でも、宅内機器と宅外機器とを区別し、コンテンツの配信契約を結んだユーザ宅内での個人使用に限定できない。

そこで本発明はかかる問題点に鑑みてなされたものであり、コンテンツをユーザ宅内での個人使用に限定するために、ユーザ宅内の機器を簡易に設定することが可能な、認証システム及び鍵登録装置を提供することを目的とする。

【0011】

【課題を解決するための手段】

上記目的を達成するために、本発明は、第1機器と第2機器との間において、認証を行う認証システムであって、前記第2機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第1鍵データを生成し、生成した第1鍵データを前記第1機器に送信する鍵登録装置と、前記鍵登録装置から前記第1鍵データを受信して記憶し、当該第1鍵データを用いて前記第2機器を認証する第1機器と、前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第2鍵データを予め記憶しており、前記第2鍵データを用いて前記第1機器による認証を受ける第2機器とから構成されることを特徴とする認証システムである。

【0012】

この構成によると、鍵登録装置を用いない限り、第1機器に第2機器の鍵を登録することは出来ないため、登録された機器以外と通信することを防ぐ。これにより、コンテンツをユーザ宅内での個人使用に限定することが出来る。また、鍵登録装置を用いることによって、簡易に第1機器に第1鍵データを設定することが出来る。

【0013】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

1. 実施の形態1

1.1 認証システム1100の構成

認証システム1100は、図1に示すように、専用端末100、宅内システム200及びコンテンツ配信装置800から構成される。また、宅内システム200は、宅内サーバ300、TV400、TV500及びルータ600から構成される。

【0014】

コンテンツをユーザに有料で提供する管理機関900は、専用端末100、及びコンテン

10

20

30

40

50

ッ配信装置 800 を有している。コンテンツ配信装置 800 は、コンテンツを記録媒体に記録して提供する。なお、宅内システム 200 とコンテンツ配信装置 800 とが、ネットワークを介して接続されている場合、コンテンツをネットワークを介して配信しても良い。

ユーザは、自宅において、宅内システム 200 を有している。

【0015】

専用端末 100 を所持しているサービスマンは、管理機関 900 の指示により、ユーザの自宅を訪問し、専用端末 100 を専用のインターフェースを介して宅内サーバ 300 に接続する。なお、専用端末 100 は、USB などの汎用のインターフェースを介して接続するようにしても良い。

専用端末 100 は、外部から TV 400 に固有の ID である、機器識別子 ID 4 の入力を受け付けると、機器識別子 ID 4 から認証鍵 Ke_N 14 を生成する。生成した認証鍵 Ke_N 14 及び機器識別子 ID 4 を宅内サーバ 300 へ送信する。宅内サーバ 300 は、機器識別子 ID 4 及び認証鍵 Ke_N 14 を対応付けて記憶する。

【0016】

一方、TV 400 は、認証鍵 Ke_N 14 を予め記憶している。ユーザが TV 400 により、コンテンツを再生する際に、宅内サーバ 300 は、TV 400 を、認証鍵 Ke_N 14 を用いて認証し、宅内サーバ 300 は、認証に成功した場合にコンテンツを TV 400 へ送信し、TV 400 は、コンテンツを受信して再生する。

こうしてユーザは、コンテンツを楽しむことが出来る。

【0017】

以下に、認証システム 1100 の各構成について詳しく説明する。

1. 1. 1 専用端末 100

専用端末 100 は、宅内サーバ 300 に TV 400 の機器識別子 ID 4 及び認証鍵 Ke_N 14 を登録するための装置である。専用端末 100 は、管理機関 900 から指示を受けたサービスマンが所持する。サービスマンは、TV 400 が宅内に存在することを確認する。確認した後、予め定められたコンテンツ保護機能を有する機器間でコンテンツを利用できるように、専用端末 100 を用いて設定する。

【0018】

専用端末 100 は図 2 に示すように、制御部 101、入力部 102、検証部 103、記憶部 104、暗号化部 105、鍵生成部 106、送受信部 107 及び認証部 108 から構成される。

以下に、各構成について説明する。

(1) 記憶部 104

記憶部 104 は、サービスマン識別子 ID # S 1、パスワード S 1 及び関数 F を記憶している。また、記憶部 104 は関数 F を用いて機器識別子 ID 4 を暗号化するための暗号化鍵 F 1 を記憶している。

【0019】

ここで、関数 F は一例として DES の暗号化アルゴリズムである。DES については公知であるので、説明を省略する。

サービスマン識別子 ID # S 1 は、専用端末 100 を利用するサービスマンに固有の ID である。パスワード S 1 は、専用端末 100 を利用するためのパスワードであり、前記サービスマンのみがこのパスワードを知っている。

【0020】

このサービスマン識別子 ID # S 1 及びパスワード S 1 によって、専用端末 100 を使用できるサービスマンを限定する。

(2) 入力部 102

入力部 102 は、サービスマンの操作により、サービスマン識別子 ID # S 1、パスワード S 1 及び機器識別子 ID 4 の入力を受け付ける。受け付けたデータを制御部 101 に出力する。

10

20

30

40

50

(3) 検証部 103

検証部 103 は、以下のようにして、専用端末 100 の使用を許可されたサービスマンであるか否かを検証する。

【0021】

検証部 103 は、制御部 101 からサービスマンのサービスマン識別子 ID # S1 及びパスワード S1 を受け取ると、記憶部 104 に記憶している ID 及びパスワードを読み出す。受け取ったサービスマン識別子 ID # S1 及びパスワード S1 と、読み出した ID 及びパスワードとが一致するか否かを検証する。検証結果を制御部 101 に出力する。

(4) 認証部 108

認証部 108 は、宅内サーバ 300 と相互認証を行う。相互認証は、一例として、共通の 10
情報を用いたチャレンジレスポンス方式で行う。ここで、チャレンジレスポンス方式については、公知であるので説明を省略する。

【0022】

認証部 108 は、認証結果を制御部 101 に出力する。

(5) 鍵生成部 106

鍵生成部 106 は、制御部 101 から機器識別子 ID 4 を受け取ると、記憶部 104 から関数 F を読み出す。読み出した関数 F を用いて機器識別子 ID 4 から認証鍵 $Ke \times 14$ を生成する。

【0023】

ここで、 $Ke \times 14 = F(F1, ID4)$ と表される。F(A, B) は、暗号化鍵 A を用 20
いて B を暗号化することを示す。

生成した認証鍵 $Ke \times 14$ を制御部 101 へ出力する。

(6) 暗号化部 105

暗号化部 105 は、暗号化鍵 E1 を有する。

【0024】

暗号化部 105 は、制御部 101 から機器識別子 ID 4 及び認証鍵 $Ke \times 14$ を受け取る。受け取った機器識別子 ID 4 及び認証鍵 $Ke \times 14$ を、暗号化アルゴリズム E に基づいて暗号化し、暗号化機器識別子 ID 4 及び暗号化認証鍵 $Ke \times 14$ を生成する。ここで、暗号化機器識別子 ID 4 = $E(E1, ID4)$ と表される。また、暗号化認証鍵 $Ke \times 14 = E(E1, Ke \times 14)$ と表される。E(A, B) は、暗号化鍵 A を用いて、B を暗 30
号化することを示す。

【0025】

暗号化アルゴリズム E は一例として RSA である。RSA は公知であるので説明を省略する。

暗号化機器識別子 ID 4 及び暗号化認証鍵 $Ke \times 14$ を制御部 101 へ出力する。(7)

送受信部 107

送受信部 107 は、宅内サーバ 300 とデータの送受信を行う。送受信部 107 は、制御部 101 から暗号化機器識別子 ID 4 及び暗号化認証鍵 $Ke \times 14$ を受け取ると、宅内サーバ 300 に送信する。

(8) 制御部 101

制御部 101 は、入力部 102 からサービスマン識別子 ID # S1 及びパスワード S1 を受け取ると、受け取ったサービスマン識別子 ID # S1 とパスワード S1 とを検証部 103 に検証させる。検証部 103 から検証結果を受け取る。検証結果が成功か否かを判断し、検証結果が失敗の場合、処理を終了する。検証結果が成功の場合、処理を継続する。

【0026】

制御部 101 は、入力部 102 から機器識別子 ID 4 を受け取ると、認証部 108 に宅内サーバ 300 との相互認証を行わせる。認証部 108 から認証結果を受け取る。受け取った認証結果が成功か否かを判断し、認証結果が失敗の場合、処理を終了する。認証結果が成功の場合、鍵生成部 106 に機器識別子 ID 4 を出力し、鍵を生成させる。鍵生成部 106 から認証鍵 $Ke \times 14$ を受け取ると、受け取った認証鍵 $Ke \times 14$ 及び機器識別子 I 50

D 4 を暗号化部 1 0 5 へ出力する。

【0 0 2 7】

暗号化部 1 0 5 から受け取る暗号化機器識別子 I D 4 及び暗号化認証鍵 K e × 1 4 を、送受信部 1 0 7 を介して宅内サーバ 3 0 0 に送信する。

1. 1. 2 宅内サーバ 3 0 0

宅内サーバ 3 0 0 は、管理機関 9 0 0 に認可された機器である。宅内サーバ 3 0 0 は、蓄積コンテンツを記憶している。専用端末 1 0 0 によって登録された鍵を用いて、T V 4 0 0 又は T V 5 0 0 を認証し、蓄積コンテンツを配信する。

【0 0 2 8】

宅内サーバ 3 0 0 は図 2 に示すように、制御部 3 0 1、認証部 3 0 2、送受信部 3 0 3、
復号部 3 0 4、記憶部 3 0 5、送受信部 3 0 6、認証部 3 0 7 及び暗号化部 3 0 8 から構成される。 10

以下、各部について説明する。

(1) 記憶部 3 0 5

記憶部 3 0 5 は、記憶領域 3 0 9 及び外部からは観測や変更が出来ない領域である記憶領域 3 1 0 から成る。

【0 0 2 9】

記憶領域 3 0 9 は、蓄積コンテンツを記憶している。

記憶領域 3 1 0 は、既に登録されている T V 5 0 0 の機器識別子 I D 5 及び認証鍵 K e × 1 5 を対応付けて記憶している。また、専用端末 1 0 0 から受け取る、T V 4 0 0 の機器
識別子 I D 4 及び認証鍵 K e × 1 4 を記憶する領域を備える。 20

(2) 送受信部 3 0 3

送受信部 3 0 3 は、専用端末 1 0 0 と物理的に接続される。また、接続された専用端末 1 0 0 とデータの送受信を行う。

(3) 認証部 3 0 2

認証部 3 0 2 は、専用端末 1 0 0 と相互認証を行う。相互認証は、一例として共通の情報を
用いたチャレンジレスポンス方式で行う。認証結果を制御部 3 0 1 に出力する。

(4) 復号部 3 0 4

復号部 3 0 4 は、制御部 3 0 1 から受け取る暗号化機器識別子 I D 4 及び暗号化認証鍵 K e × 1 4 を、復号アルゴリズム D に従って復号し、機器識別子 I D 4 及び認証鍵 K e × 1 4 を生成する。ここで、復号アルゴリズム D は、暗号化アルゴリズム E の逆の処理を行う。
。 30

【0 0 3 0】

復号部 3 0 4 は、機器識別子 I D 4 及び認証鍵 K e × 1 4 を制御部 3 0 1 へ出力する。

(5) 送受信部 3 0 6

送受信部 3 0 6 は、ルータ 6 0 0 を介して T V 4 0 0 又は 5 0 0 とデータの送受信を行う。
。

(6) 認証部 3 0 7

認証部 3 0 7 は、T V 4 0 0 にコンテンツを配信する際、機器識別子 I D 4 と認証鍵 K e × 1 4 を用いて T V 4 0 0 の認証及びセッション鍵の共有を行う。 40

【0 0 3 1】

認証及びセッション鍵共有の一例として以下の方法がある。

認証部 3 0 7 は、乱数 r 1 を生成し、T V 4 0 0 に送信する。その後、T V 4 0 0 から、
r 1 と、T V 4 0 0 が生成した乱数 r 2 とを結合したデータ r 1 r 2 を、認証鍵 K e × 1 4 を用いて暗号化した暗号化 r 1 r 2 を受信する。受信した暗号化 r 1 r 2 を復号する。
復号文からもとの r 1 が導出されることにより、T V 4 0 0 を認証する。

【0 0 3 2】

また、このとき導出された r 2 をセッション鍵として暗号化部 3 0 8 へ出力する。

認証部 3 0 7 は、T V 5 0 0 にコンテンツを配信する際も同様の認証及びセッション鍵の共有を行う。

(7) 暗号化部 308

暗号化部 308 は、記憶領域 309 に記憶しているコンテンツを暗号化する。

【0033】

TV400 へ配信するコンテンツは、認証部 307 で TV400 を認証した際に導出されたセッション鍵 K_2 を用いて暗号化し、暗号化コンテンツを生成する。暗号化コンテンツを、制御部 301 へ出力する。

TV500 へ配信するコンテンツも、同様に導出したセッション鍵を用いて暗号化する。

(8) 制御部 301

制御部 301 は、専用端末 100 が接続されると、認証部 302 に相互認証を行わせる。認証部 302 から認証結果を受け取る。認証結果が成功か否かを判断する。認証結果が失敗の場合、処理を終了する。認証結果が成功の場合、処理を継続する。制御部 301 は、送受信部 303 を介して専用端末 100 から暗号化機器識別子 ID4 及び暗号化認証鍵 $K_{e \times 14}$ を受け取る。受け取った暗号化機器識別子 ID4 及び暗号化認証鍵 $K_{e \times 14}$ を復号部 304 に出力し、復号させる。

【0034】

制御部 301 は、復号部 304 から復号した機器識別子 ID4 及び認証鍵 $K_{e \times 14}$ を受け取る。受け取った機器識別子 ID4 及び認証鍵 $K_{e \times 14}$ を対応付けて、記憶領域 310 に書き込む。

制御部 301 は、TV400 にコンテンツを配信する場合、認証部 307 で TV400 の認証を行わせる。認証部 307 から認証結果を受け取ると、認証結果が成功か否かを判断する。認証結果が失敗の場合、コンテンツの配信を終了する。認証結果が成功の場合、暗号化部 308 にコンテンツを暗号化させる。暗号化部 308 から暗号化コンテンツを受け取ると、送受信部 306 を介して TV400 へ配信する。

また、TV500 へコンテンツを配信する場合も同様の処理を行う。

1. 1. 3 TV400, 500

TV400, 500 は、予め管理機関 900 に認可された機器である。

【0035】

TV400 は、外部から見ることが出来る場所に、管理機関 900 が設定した、TV400 に固有の機器識別子 ID4 が付されている。

TV400 は図 3 に示すように、制御部 401、認証部 402、送受信部 403、復号部 407、記憶部 404、モニタ 405 及びスピーカ 406 から構成される。また、TV500 も同様の構成である。なお、図 3 では簡単のため、宅内サーバ 300 と、ルータ 600 と、TV400 とを一例にして示す。

【0036】

以下、各構成について説明する。

(1) 記憶部 404

記憶部 404 は、外部から観測や変更が出来ない記憶領域である。記憶部 404 は、TV400 に固有の機器識別子 ID4 及び認証鍵 $K_{e \times 14}$ を記憶している。認証鍵 $K_{e \times 14}$ は、機器識別子 ID4 から秘密の関数 F を用いて生成したものである。(2) 認証部 402

認証部 402 は、宅内サーバ 300 と相互認証を行う。

【0037】

認証部 402 は、送受信部 403 を介して乱数 r_1 を受け取ると、記憶部 404 から認証鍵 $K_{e \times 14}$ を読み出す。認証部 402 は、乱数 r_2 を生成する。受け取った r_1 と生成した r_2 とを結合する。結合したデータ $r_1 r_2$ を、読み出した認証鍵 $K_{e \times 14}$ を用いて暗号化し、暗号化 $r_1 r_2$ を生成する。暗号化 $r_1 r_2$ を送受信部 403 を介して宅内サーバ 300 に送る。

【0038】

認証部 402 は、生成した乱数 r_2 をセッション鍵として復号部 407 に出力する。

認証部 402 は、認証結果を制御部 401 へ出力する。

10

20

30

40

50

(3) 復号部 407

復号部 407 は、送受信部 403 を介して暗号化コンテンツを受け取る。受け取った暗号化コンテンツを、認証部 402 で生成したセッション鍵 K2 を用いて復号する。復号したコンテンツを制御部 401 に出力する。

(4) モニタ 405

モニタ 405 は、制御部 401 から受け取る画像データを再生する。

(5) スピーカ 406

スピーカ 406 は、制御部 401 から受け取る音声データを再生する。

(6) 送受信部 403

送受信部 403 は、ルータ 600 を介して、宅内サーバ 300 と、データの送受信を行う。 10

(7) 制御部 401

制御部 401 は、認証部 402 に、送受信部 403 を介して宅内サーバ 300 との相互認証を行わせる。認証部 402 から認証結果を受け取ると、認証結果が成功か否かを判断する。認証結果が失敗の場合、処理を終了する。

【0039】

制御部 401 は、送受信部 403 を介して宅内サーバ 300 から受信する暗号化コンテンツを、復号部 407 に復号させる。復号部 407 から復号されたコンテンツを受け取ると、モニタ 405 及びスピーカ 406 へ出力する。

1. 2 認証システム 1100 の動作 20

1. 2. 1 専用端末 100 を用いて宅内サーバ 300 に TV 400 を登録する場合の動作

以下、図 4 を用いて、専用端末 100 を保持したサービスマンが宅内システム 200 の宅内サーバ 300 に、TV 400 を登録する際の動作を説明する。ただし、宅内サーバ 300 には、既に TV 500 が登録されている。

【0040】

サービスマンは、専用端末 100 を保持してユーザの宅内へ行く。コンテンツの利用が、個人使用の範囲として許容される場合、サービスマンは、TV 400 が宅内にあることを確認して、登録の処理を行う。

サービスマンは、宅内サーバ 300 に登録を行う前に、入力部 102 からサービスマンのサービスマン識別子 ID#S1 及びパスワード S1 を入力する。専用端末 100 の制御部 101 は、入力部 102 で入力を受け付けると、検証部 103 に検証させる。制御部 101 は、検証部 103 から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。 30

【0041】

専用端末 100 は、サービスマンにより宅内サーバ 300 に接続される。制御部 101 は、入力部 102 が機器識別子 ID4 の入力を受け付けると（ステップ S1）、認証部 108 に、宅内サーバ 300 と相互認証を行わせる（ステップ S2）。制御部 101 は、認証部 108 から認証結果を受け取ると、認証結果が成功か否かを判断する（ステップ S3）。認証結果が失敗の場合（ステップ S3 で NO）、処理を終了する。認証結果が成功の場合（ステップ S3 で YES）、鍵生成部 106 に鍵を生成させる（ステップ S4）。制御部 101 は、鍵生成部 106 から生成された認証鍵 KeY14 を受け取ると、機器識別子 ID4 及び認証鍵 KeY14 を、暗号化部 105 に暗号化させる（ステップ S5）。制御部 101 は、暗号化機器識別子 ID4 及び暗号化認証鍵 KeY14 を、送受信部 107 を介して宅内サーバ 300 に送信する（ステップ S6）。 40

1. 2. 2 宅内サーバ 300 が鍵を登録する場合の動作

宅内サーバ 300 が、専用端末 100 から受信した情報を書き込む際の動作を、図 5 を用いて説明する。

【0042】

宅内サーバ 300 の制御部 301 は、認証部 302 で専用端末 100 と相互認証を行う（ 50

ステップS11)。制御部301は、認証部302から認証結果を受け取ると、成功か否かを検証し(ステップS12)、検証結果が失敗の場合(ステップS12でNO)、処理を終了する。検証結果が成功の場合(ステップS12でYES)、専用端末100からデータが送信されるのを待つ。

【0043】

制御部301は、専用端末100から送受信部303を介して、暗号化機器識別子ID4及び暗号化認証鍵Ke_N14を受信する(ステップS13)。暗号化機器識別子ID4及び暗号化認証鍵Ke_N14を復号部304で復号させる(ステップS14)。復号した機器識別子ID4及び認証鍵Ke_N14を対応付けて、記憶領域310に書き込む(ステップS15)。

1. 2. 3 宅内サーバ300がTV400にコンテンツを配信する際の動作

宅内サーバ300が、TV400にコンテンツを配信する際の動作を、図6を用いて説明する。

【0044】

宅内サーバ300の制御部301は、認証部307にTV400を認証させる(ステップS21)。

制御部301は、認証部307から認証結果を受け取り、認証結果が成功か否かを判断する(ステップS22)。認証結果が失敗の場合(ステップS22でNO)、処理を終了する。認証結果が成功の場合(ステップS22でYES)、記憶領域309に記憶している蓄積コンテンツを読み出す(ステップS23)。読み出したコンテンツを、認証の際に導出したセッション鍵を用いて暗号化部308で暗号化する(ステップS24)。暗号化したコンテンツを送受信部306を介してTV400に配信する(ステップS25)。

1. 2. 4 宅内サーバ300がTV400の認証を行う際の動作

宅内サーバ300がTV400の認証を行う動作(ステップS21)を、図7を用いて説明する。

【0045】

宅内サーバ300の認証部307は、乱数r1を生成する(ステップS31)。生成した乱数r1を送受信部306を介してTV400に送信する(ステップS32)。

TV400の認証部402は、送受信部403を介して乱数r1を受け取ると、乱数r2を生成する(ステップS33)。受け取ったr1と生成したr2を結合し(ステップS34)、結合したr1r2を、認証鍵Ke_N14を用いて暗号化する(ステップS35)。暗号化r1r2を送受信部403を介して宅内サーバ300へ送信する(ステップS36)。

【0046】

宅内サーバ300の認証部307は、受け取った暗号化r1r2を認証鍵Ke_N14を用いて復号し、r1r2を導出する(ステップS37)。復号したデータから、r1が導出されたか否かを判断する(ステップS38)。r1が導出されなかった場合(ステップS38でNO)、認証が失敗であることを示す認証結果を制御部301へ出力する(ステップS40)。r1が導出された場合(ステップS38でYES)、暗号化部308へr2を出力する(ステップS39)。また、認証部307は、認証が成功であることを示す認証結果を制御部301へ出力する(ステップS40)。

2. 実施の形態2

実施の形態1の方法では、鍵を登録した専用端末をサービスマンが紛失したときなど、不正に使用される可能性がある場合に、紛失前に登録されたものと、紛失後に登録されたものとが区別できないという問題がある。そこで、不正に使用される可能性がある専用端末で登録した鍵を無効化することが出来る認証システム1200について説明する。

2. 1 認証システム1200の構成

認証システム1200は、図8に示すように、専用端末120、140、宅内システム220、インターネット700、管理装置920及びコンテンツ配信装置800から構成される。また、宅内システム220は、宅内サーバ320、TV420、TV520及びル

10

20

30

40

50

ータ620から構成される。

【0047】

管理装置920及びコンテンツ配信装置800は、インターネット700を経由して、ルータ620に接続されている。

以下、認証システム1100と異なる構成について説明する。

2.1.1 管理装置920

管理装置920は、無効化情報を発行する。無効化情報は、不正利用される可能性がある専用端末及び当該専用端末で登録された鍵を無効化するための情報である。無効化情報は、無効化される専用端末に固有のIDと、IDに対してデジタル署名アルゴリズムSを施して生成したデジタル署名データから構成される。ここで、デジタル署名アルゴリズムSは、一例として、有限体上の離散対数問題を安全性の根拠とするEIGamal署名方式に基づくものである。この有限体上のEIGamal署名方式については、公知であるので説明を省略する。

10

2.1.2 専用端末120

専用端末120は図15に示すように、制御部121、入力部122、検証部123、記憶部124、暗号化部125、鍵生成部126、送受信部127及び認証部128から構成される。入力部122、検証部123、鍵生成部126、送受信部127及び認証部128は、専用端末100と同様の構成である。

【0048】

以下、専用端末100と異なる構成の記憶部124、暗号化部125及び制御部121について説明する。

20

(1) 記憶部124

記憶部124は、関数F、サービスマン識別子ID#S2、パスワードS2及び、専用端末120に固有のIDであるModule-2を記憶している。

(2) 暗号化部125

暗号化部125は、制御部121から機器識別子ID4、認証鍵Ke×24及びModule-2を受け取る。受け取った機器識別子ID4、認証鍵Ke×24及びModule-2を、暗号化アルゴリズムEに基づいて暗号化し、暗号化機器識別子ID4、暗号化認証鍵Ke×24及び暗号化Module-2を生成する。暗号化部125は、暗号化機器識別子ID4、暗号化認証鍵Ke×24及び暗号化Module-2を制御部121へ出力する。

30

(3) 制御部121

制御部121は、専用端末100の制御部101と同様に、検証部123にサービスマンのID及びパスワードを検証させ、認証部128に宅内サーバ320との相互認証を行わせ、鍵生成部126に鍵を生成させる。

【0049】

制御部121は、鍵生成部126から認証鍵Ke×24を受け取ると、記憶部124からModule-2を読み出す。機器識別子ID4及び受け取った認証鍵Ke×24と読み出したModule-2とを暗号化部125に暗号化させる。

暗号化部125から暗号化機器識別子ID4、暗号化認証鍵Ke×24及び暗号化Module-2を受け取ると、送受信部127を介して宅内サーバ320へ送信する。

40

2.1.3 専用端末140

専用端末140は図16に示すように、制御部141、入力部142、検証部143、記憶部144、暗号化部145、鍵生成部146、送受信部147及び認証部148から構成される。

【0050】

入力部142、検証部143、暗号化部145、送受信部147及び認証部148は、専用端末120と同様の構成のため、説明を省略する。

以下、専用端末120と異なる記憶部144、鍵生成部146及び制御部141について説明する。

50

(1) 記憶部 144

記憶部 144 は、関数 F と異なる関数 G、サービスマン識別子 ID#S3、パスワード S3 及び専用端末 140 に固有の ID である Module-3 を記憶している。

(2) 鍵生成部 146

鍵生成部 146 は、制御部 141 から機器識別子 ID4 を受け取ると、記憶部 144 から関数 G を読み出す。読み出した関数 G を用いて機器識別子 ID4 から認証鍵 Ke×34 を生成する。生成した認証鍵 Ke×34 を制御部 141 へ出力する。機器識別子 ID5 を受け取った場合も同様に処理し、認証鍵 Ke×35 を制御部 141 へ出力する。

(3) 制御部 141

制御部 141 は、制御部 121 と同様に、検証部 143 にサービスマン識別子 ID#S3 及びパスワード S3 を検証させ、認証部 148 に宅内サーバ 320 との相互認証を行わせ、鍵生成部 146 に鍵を生成させる。 10

【0051】

制御部 141 は、鍵生成部 146 から認証鍵 Ke×34 を受け取ると、記憶部 144 から Module-3 を読み出す。機器識別子 ID4 及び受け取った認証鍵 Ke×34 と読み出した Module-3 とを暗号化部 145 に暗号化させる。

暗号化部 145 から暗号化機器識別子 ID4、暗号化認証鍵 Ke×34 及び暗号化 Module-3 を受け取ると、送受信部 147 を介して宅内サーバ 320 へ送信する。

2. 1. 4 宅内サーバ 320

宅内サーバ 320 は図 17 に示すように、制御部 321、認証部 322、送受信部 323、復号部 324、記憶部 325、送受信部 326、認証部 327、暗号化部 328 及び署名検証部 329 から構成される。 20

【0052】

以下、宅内サーバ 300 と異なる構成である記憶部 325、署名検証部 329 及び制御部 321 について説明する。

(1) 記憶部 325

記憶部 325 は、図 9 に示すように、記憶領域 332 及び外部から観測や変更が出来ない領域である記憶領域 330 と記憶領域 331 とから成る。

【0053】

記憶領域 332 は、コンテンツ配信装置 800 から配信される蓄積コンテンツを記憶する領域である。 30

記憶領域 331 は、管理装置 920 の公開鍵を記憶している。

記憶領域 330 は図 9 に示すように、記憶領域 333 と 334 とから成る。

記憶領域 334 は、無効化された専用端末の ID を記憶する領域である。

【0054】

記憶領域 333 は、既に宅内サーバ 320 に登録されている TV520 の機器識別子 ID5、認証鍵 Ke×25、Module-2 及び無効化フラグを対応付けて記憶している。Module-2 は、認証鍵 Ke×25 を登録した専用端末 120 の ID である。無効化フラグは、認証鍵 Ke×25 を登録した専用端末及び当該専用端末を用いて登録された鍵が無効化されているか否かを示すフラグである。図 9 では破線で囲んで示している。本実施の形態 2 では、無効化フラグが「1」の場合、対応付けられている ID が示す専用端末及び当該専用端末を用いて登録した鍵は無効化されていることを示し、「0」の場合、無効化されていないことを示す。 40

【0055】

記憶領域 333 は、制御部 321 から受け取る機器識別子 ID4、認証鍵 Ke×24 及び Module-2 を無効化フラグの「0」と対応付けて、図 10 に示すように、記憶する。

(2) 署名検証部 329

署名検証部 329 は、制御部 321 から無効化情報を受け取る。受け取った無効化情報の管理機関 900 の署名データに署名検証 V を施して検証する。ここで、署名検証 V は、前 50

記デジタル署名アルゴリズム S により生成された署名データを検証するアルゴリズムである。検証結果を制御部 321 へ出力する。

(3) 制御部 321

制御部 321 は、専用端末 120 から暗号化機器識別子 ID4、暗号化認証鍵 Ke₂₄ 及び暗号化 Module-2 を受け取り、制御部 301 と同様に、復号部 324 で復号する。復号部 324 から機器識別子 ID4、認証鍵 Ke₂₄ 及び Module-2 を受け取ると、これらと無効化フラグの「0」とを対応付けて、図 10 に示すように、記憶領域 333 に書き込む。

【0056】

制御部 321 は、ルータ 620 を介して管理装置 920 から無効化情報を受信すると、署名検証部 329 に署名検証させる。署名検証部 329 から検証結果を受け取ると、検証結果が正しいか否かを判断する。検証結果が正しくない場合、処理を終了する。検証結果が正しい場合、受け取った無効化情報に含まれる無効化される専用端末の ID を、図 11 に示すように、記憶領域 334 に記憶する。また、記憶領域 333 に記憶している鍵と対応付けて記憶している Module-2 が、無効化情報に含まれる ID と一致するか否かを判断する。一致する場合、Module-2 と対応付けて記憶している無効化フラグ「0」を、図 11 に示すように、「1」に書き換える。このように、無効化フラグ「1」と対応付けて記憶している認証鍵 Ke₂₄ 及び認証鍵 Ke₂₅ は、無効化されたことを示す。

【0057】

また、制御部 321 は、Module-2 と対応付けて記憶している認証鍵 Ke₂₄ が無効化されたことを通知する認証鍵無効化情報を、送受信部 326 を介して TV420 及び TV520 に送信する。認証鍵無効化情報は、無効化された Module-2 と対応付けて記憶している認証鍵 Ke₂₄ が無効化されたことを、TV420 及び TV520 に通知するものであり、無効化された認証鍵 Ke₂₄ を含む。

2. 1. 5 TV420、520

TV420、520 は、予め管理機関 900 に認可された機器である。

【0058】

TV420 は図 18 に示すように、制御部 421、認証部 422、送受信部 423、復号部 427、記憶部 424、モニタ 425 及びスピーカ 426 から構成される。また、TV520 も同様の構成であり、図 19 に示すように、制御部 521、認証部 522、送受信部 523、記憶部 524、モニタ 525、スピーカ 526 及び復号部 527 から構成される。送受信部 423、復号部 427、モニタ 425 及びスピーカ 426 は、TV400 と同様の構成である。以下、TV400 と異なる構成である記憶部 424、認証部 422 及び制御部 421 について説明する。

(1) 記憶部 424

記憶部 424 は、外部から観測や変更が出来ない記憶領域である。記憶部 424 は、TV420 に固有の機器識別子 ID4、認証鍵 Ke₂₄ 及び認証鍵 Ke₃₄ を記憶している。認証鍵 Ke₂₄ は、機器識別子 ID4 から関数 F を用いて生成した鍵である。認証鍵 Ke₃₄ は、機器識別子 ID4 から関数 G を用いて生成した鍵である。認証鍵 Ke₂₄ 及び認証鍵 Ke₃₄ には、予め優先順位が決められている。認証鍵 Ke₂₄ は、認証鍵 Ke₃₄ より優先順位が上位であり、先に利用される。

【0059】

TV520 の記憶部 524 も同様に、機器識別子 ID5、認証鍵 Ke₂₅ 及び認証鍵 Ke₃₅ を記憶している。認証鍵 Ke₂₅ は、機器識別子 ID5 から関数 F を用いて生成したものであり、認証鍵 Ke₃₅ は、機器識別子 ID5 から関数 G を用いて生成したものである。認証鍵 Ke₂₅ 及び認証鍵 Ke₃₅ にも、優先順位が決められている。

(2) 認証部 422

認証部 422 が認証部 402 と異なる部分について説明する。

【0060】

10

20

30

40

50

認証部 422 は、宅内サーバ 320 により認証を受けるとき、優先順位が上位の認証鍵 $Ke \times 24$ を先に用いて、 $r1r2$ を暗号化する。認証鍵 $Ke \times 24$ が無効化された場合は、次の優先順位の認証鍵 $Ke \times 34$ を用いる。

(3) 制御部 421

制御部 421 は、送受信部 423 を介して宅内サーバ 320 から認証鍵無効化情報を受信すると、記憶部 424 に記憶している認証鍵 $Ke \times 24$ 又は認証鍵 $Ke \times 34$ の何れかと一致するか否かを判断する。一致する場合、一致した認証鍵を削除する。

2.2 認証システム 1200 の動作

2.2.1 専用端末 120 を用いて宅内サーバ 320 に TV420 を登録する場合の動作

宅内サーバ 320 と TV520 とが、ルータ 620 で接続されている宅内システム 220 に、サービスマンが新たに TV420 を接続して、宅内サーバ 320 に鍵を設定する際の動作を説明する。ただし、TV520 の鍵認証鍵 $Ke \times 25$ は、宅内サーバ 320 にすでに登録されている。

【0061】

サービスマンは、専用端末 120 を保持してユーザ宅内へ行く。サービスマンは、登録処理を行う前に、専用端末 120 に、サービスマン識別子 ID#82 及びパスワード 82 を入力する。

専用端末 120 の制御部 121 は、入力部 122 からサービスマンのサービスマン識別子 ID#82 及びパスワード 82 の入力を受け付けると、専用端末 100 と同様に、検証部 123 に検証させる。制御部 121 は、検証部 123 から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。

【0062】

専用端末 120 は、サービスマンにより、宅内サーバ 320 に接続される。制御部 121 は、入力部 122 で機器識別子 ID4 の入力を受け付けると、実施の形態 1 と同様の動作で認証鍵 $Ke \times 24$ を生成する。制御部 121 は、鍵生成部 126 から認証鍵 $Ke \times 24$ を受け取ると、記憶部 124 から Module-2 を読み出す。機器識別子 ID4、認証鍵 $Ke \times 24$ 及び Module-2 を暗号化部 125 へ出力する。

【0063】

暗号化部 125 は、受け取った機器識別子 ID4、認証鍵 $Ke \times 24$ 及び Module-2 を、暗号化アルゴリズム E に基づいて暗号化する。暗号化部 125 は、暗号化機器識別子 ID4、暗号化認証鍵 $Ke \times 24$ 及び暗号化 Module-2 を制御部 121 へ出力する。

制御部 121 は、受け取った暗号化機器識別子 ID4、暗号化認証鍵 $Ke \times 24$ 及び暗号化 Module-2 を、送受信部 127 を介して宅内サーバ 320 へ送信する。

【0064】

宅内サーバ 320 の制御部 321 は、送受信部 323 を介して暗号化機器識別子 ID4、暗号化認証鍵 $Ke \times 24$ 及び暗号化 Module-2 を受け取ると、実施の形態 1 と同様に復号部 324 に復号させる。

制御部 321 は、復号部 324 から復号した機器識別子 ID4、認証鍵 $Ke \times 24$ 及び Module-2 を受け取ると、記憶領域 334 から無効化した専用端末の ID を読み出す。読み出した ID と、復号した ID とが一致するか否かを判断する。一致する場合、処理を終了する。一致しない場合又は記憶領域 334 に ID が記憶されていない場合、制御部 321 は、図 10 に示すように、Module-2 と機器識別子 ID4 と認証鍵 $Ke \times 24$ と無効化フラグ「0」と対応付けて記憶領域 333 に書き込む。

2.2.2 専用端末 120 が無効化された場合の動作

専用端末 120 が、紛失等不正に利用される可能性がある場合に、専用端末 120 を無効化する動作を、図 13 を用いて説明する。

【0065】

10

20

30

40

50

管理装置 920 は、無効化情報をインターネット 700 を介して、宅内サーバ 320 に配信する。

宅内サーバ 320 の制御部 321 は、ルータ 620 及び送受信部 326 を介して無効化情報を受信する（ステップ S41）。受信した無効化情報の署名データを署名検証部 329 で検証する（ステップ S42）。

【0066】

制御部 321 は、署名検証部 329 から検証結果を受け取る。受け取った検証結果が正しいか否かを判断する（ステップ S43）。検証結果が正しくない場合（ステップ S43 で NO）、処理を終了する。検証結果が正しい場合（ステップ S43 で YES）、図 11 に示すように、無効化情報に含まれる専用端末 120 の ID である Module-2 を記憶領域 334 に書き込む（ステップ S44）。また、記憶領域 333 に記憶している鍵認証鍵 Ke\times24 及び認証鍵 Ke\times25 を生成した専用端末 120 の ID である Module-2 を読み出す（ステップ S45）。読み出した Module-2 と、無効化情報に含まれる ID とが一致するか否かを判断する（ステップ S46）。一致しない場合（ステップ S46 で NO）、処理を終了する。一致する場合（ステップ S46 で YES）、図 11 に示すように、記憶領域 333 に記憶している Module-2 を用いて登録した認証鍵 Ke\times24 及び認証鍵 Ke\times25 を無効化するため、対応して記憶している無効化フラグを「1」に書き換える（ステップ S47）。

【0067】

また、制御部 321 は、認証鍵 Ke\times24 が無効化されたことを通知する認証鍵無効化情報を、送受信部 326 を介して TV420 及び TV520 に送信する。

このように、宅内サーバ 320 は、無効化された専用端末 120 の ID である Module-2 を登録することで、無効化された専用端末 120 からの接続を拒否する。また、認証鍵 Ke\times24 及び認証鍵 Ke\times25 を無効化することで、専用端末 120 を用いて不正に設定されても、不正に設定された TV との認証及びコンテンツの利用を拒否する。

2. 2. 3 専用端末 140 で TV420 及び TV520 を再登録する場合の動作

関数 F で生成された鍵認証鍵 Ke\times24 及び認証鍵 Ke\times25 が無効化された後、サービスマンが、TV420 及び TV520 のもう一つの鍵認証鍵 Ke\times34 及び認証鍵 Ke\times35 を、別の専用端末 140 を用いて再登録する。

【0068】

サービスマンは、専用端末 140 を保持してユーザ宅内へ行く。サービスマンは、登録処理を行う前に、専用端末 140 に、サービスマン識別子 ID#S3 及びパスワード S3 を入力する。

専用端末 140 の制御部 141 は、入力部 142 からサービスマンのサービスマン識別子 ID#S3 及びパスワード S3 の入力を受け付けると、専用端末 100 と同様に、検証部 143 に検証させる。制御部 141 は、検証部 143 から検証結果を受け取ると、検証結果が成功か否かを判断する。検証結果が失敗の場合、登録処理を終了する。検証結果が成功の場合、登録処理を継続する。

【0069】

専用端末 140 は、サービスマンにより、宅内サーバ 320 に接続される。制御部 141 は、入力部 142 で機器識別子 ID4 の入力を受け付けると、専用端末 100 と同様の動作で、関数 G を用いて鍵認証鍵 Ke\times34 を生成する。制御部 141 は、暗号化部 145 で専用端末 140 の ID である Module-3、機器識別子 ID4、生成した鍵認証鍵 Ke\times34 を暗号化させる。暗号化 Module-3、暗号化機器識別子 ID4 及び暗号化認証鍵 Ke\times34 を、送受信部 147 を介して宅内サーバ 320 に送信する。制御部 141 は、機器識別子 ID5 の入力を受け付けた場合も、同様に処理する。

【0070】

宅内サーバ 320 の制御部 321 は、受け取った情報を復号部 324 で復号する。制御部 321 は、復号部 324 から受け取る Module-3、機器識別子 ID4 及び認証鍵 Ke\times34 と、無効化フラグ「0」とを対応付けて、図 12 に示すように、記憶領域 333

10

20

30

40

50

に書き込む。同様に、Module-3、機器識別子ID5及び認証鍵KeX35と、無効化フラグ「0」とを対応付けて、図12に示すように、記憶領域333に書き込む。

3. 実施の形態3

実施の形態2の認証システム1200で鍵を再登録する際など、登録するTVが宅内にあり、管理機関900から認可を受けていることを確認できる場合、サービスマンが宅内で設定せず、ネットワークを介して設定しても良い。

【0071】

以下、専用端末140でインターネット700を介して、宅内サーバ320に鍵を設定する場合の構成について説明する。

3. 1 認証システム1300の構成

認証システム1300は、図14に示すように、専用端末120、140、宅内システム220、インターネット700、管理装置920及びコンテンツ配信装置800から構成される。また、宅内システム220は、宅内サーバ320、TV420、TV520及びルータ620から構成される。

【0072】

管理装置920、コンテンツ配信装置800及び専用端末140は、インターネット700を経由して、ルータ620に接続されている。

以下、認証システム1200と異なる構成について説明する。

3. 2 認証システムの動作

3. 2. 1 専用端末140で鍵を再登録する場合の動作

実施の形態2の方法で、専用端末120が無効化された後、宅内サーバ320に、インターネット700を介して専用端末140を用いてTV420の認証鍵KeX34及びTV520の認証鍵KeX35を再登録する場合の動作について説明する。

【0073】

管理機関900は、ユーザから電話で、TV420の機器識別子ID4を知らせてもらう。なお、ID4を知らせてもらう方法は、電話に限らず電子メールなどでも良い。

サービスマンは、サービスマン識別子ID#S3及びパスワードS3を入力部142から入力する。

【0074】

制御部141は、実施の形態2と同様にサービスマンのサービスマン識別子ID#S3及びパスワードS3を検証する。

専用端末140は、サービスマンによってインターネット700に接続されると、実施の形態1と同様の方法で、宅内サーバ320と相互認証を行う。相互認証が成功した場合、専用端末140と宅内サーバ320とを接続する安全な通信路を確保する。安全な通信路は、一例として、IPSec (IP Security) といった手法により、通信路上のデータが暗号化されていることで実現される。

【0075】

管理機関900で、サービスマンは、専用端末140の入力部142から機器識別子ID4を入力する。

専用端末140の制御部141は、入力部142から機器識別子ID4の入力を受け付けると、専用端末120と同様の動作で、関数Gを用いて認証鍵KeX34を生成する。制御部141は、暗号化部145でModule-3、機器識別子ID4、生成した認証鍵KeX34を暗号化させる。制御部141は、暗号化Module-3、暗号化機器識別子ID4及び暗号化認証鍵KeX34を、インターネット700を介して、宅内サーバ320に送信する。制御部141は、機器識別子ID5の入力を受け付けた場合も、同様に処理する。

【0076】

宅内サーバ320の制御部321は、暗号化Module-3、暗号化機器識別子ID4及び暗号化認証鍵KeX34を受け取ると、復号部324に復号させる。復号されたModule-3、機器識別子ID4及び認証鍵KeX34と、無効化フラグ「0」とを対応

10

20

30

40

50

付けて、記憶領域 333 に書き込む。また、暗号化 Module-3、暗号化機器識別子 ID5 及び暗号化認証鍵 Key35 を受け取ると、同様に復号し、Module-3、機器識別子 ID5 及び認証鍵 Key35 と、無効化フラグ「0」とを対応付けて、記憶領域 333 に書き込む。

【0077】

このように、専用端末 140 で、インターネット 700 を介して、宅内サーバ 320 に鍵を設定することが可能である。

4. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 無効化情報は、インターネットを介して配信されるとしたが、DVD や CD 等の蓄積メディア媒体に記録されて通知されるようにしても良い。

【0078】

また、この方法では、宅内サーバが、外部への接続手段を持たなくても実現できる。

(2) 無効化された鍵を無効化フラグ「1」と対応付けて記憶するとしたが、これに限定されない。無効化された専用端末で登録された機器の ID 及び鍵が削除される等、利用できない状態にすれば良い。

(3) 実施の形態 3 で、鍵を宅内サーバに再登録する際を例として説明したが、これに限らない。

【0079】

宅内サーバに登録する機器が宅内にあり、管理機関 900 に認可された機器であることを確認できれば、新しく登録する場合でも良い。宅内にあることを確認する方法の一例として、ユーザが機器を購入する際に、ユーザ登録カードとして、購入する機器を管理機関 900 に登録しておき、これを利用する方法がある。また、機器の ID の一部が TV であることを示す等、何れの機器であるか判断できる場合は、管理機関 900 から認可されている機種であることを確認することが出来る。また、ID の一部が、管理機関 900 から認可されていることを示すようにしても良い。

(4) 実施の形態 3 で、安全な通信路を IPsec としたが、これに限定されず、一般的な VPN (Virtual Private Network) としてもよい。また、専用線を用いて物理的に安全であっても良い。

(5) 実施の形態 3 で、専用端末 140 が暗号化したデータを宅内サーバ 320 に送信するとしたが、宅内サーバ 320 がルータ 620 を介して、専用端末 140 にデータを取りに行く構成であっても良い。

(6) 専用端末は、IC カードを PDA 又は携帯電話に接続したものであっても良い。この場合、関数 F、G など、ID と鍵の対応関係を IC カードが記憶している。

(7) 本実施の形態では、サービスマンが入力部から TV の ID を入力するとしたが、ID がバーコードとして TV に付されており、それを専用端末で読み取るようにしても良い。また、IC チップ等に記録されており、専用端末で読み取るようにしても良い。

(8) ID から鍵を生成する方法として、関数 F 又は関数 G を用いるとしたが、ID と鍵の対応関係を示すものであれば関数でなくとも良い。例えば、専用端末は、ID と鍵との対応表を記憶している構成であっても良い。

(9) 宅内サーバに鍵を登録する機器は、TV でなくとも良い。他の画像再生機器であっても良いし、音声再生機であっても良い。また、DVD やメモ리카ード等の蓄積メディアに書き込みを行う記録機器であっても良い。

【0080】

宅内サーバは、DVD 等の蓄積メディアの再生機器であっても良い。

(10) 本実施の形態では、宅内サーバが、一つの TV にコンテンツを配信する方法を記述したが、同時に複数の TV にコンテンツを配信するようにしても良い。

TV 400 と TV 500 にコンテンツを配信する際の相互認証の一例として、以下のような方法がある。

10

20

30

40

50

【0081】

まず、実施の形態1と同様の方法で、それぞれのTVと相互認証を行う。次に、宅内サーバはコンテンツを暗号化するためのコンテンツ鍵を生成する。これを各TVとそれぞれ共有したセッション鍵で暗号化して、暗号化コンテンツと共にそれぞれのTVに配信する。TVは、暗号化コンテンツを、宅内サーバと共有したセッション鍵で復号する。復号したコンテンツ鍵で暗号化コンテンツを復号し、再生する。

【0082】

これにより、複数のTVで同時にコンテンツを再生することが出来る。

(11) 本実施の形態では、宅内サーバがTV400を認証するとしたが、宅内サーバとTVとが相互認証を行う構成であっても良い。

(12) 本実施の形態2、3で、TVは関数Fを用いて生成した鍵と、関数Gを用いて生成した鍵の2つを持つとしたが、鍵は3個以上でも良い。この場合、それぞれの鍵は、それぞれ別の関数を用いて、IDから生成されたものである。

(13) 宅内サーバとTVは、ルータを介してイーサネット（登録商標）で接続されるとしたが、これに限らない。ローカルに設定されたシステムであっても良いし、ルータを用いなくても良い。

(14) 宅内サーバからコンテンツの配信を禁止する対象としては、PCだけではなく、記録機器にも配信を禁止することが出来る。

【0083】

また、上記の場合、以下に示すように送信制御をコンテンツの種類によって行っても良い

宅内サーバは、登録する機器のIDや鍵と共に、その機器が視聴だけを目的とした機器であるか、記録を行うことを目的とした機器であるか、といった機器の種類を記憶しておく。そして、別途コンテンツに付加されているコピーコントロール情報を元にして、機器への配信を許可又は禁止する。ここで、コピーコントロール情報は、一般的に(1)COPY Never、1回もコピーしてはいけない、(2)COPY Once、1回だけコピーしても良い、(3)COPY Free、自由にコピーしても良い、の3つの状態を区別する。宅内サーバは、コンテンツに付加されているコピーコントロール情報が(2)又は(3)の場合、記録機器へ配信可能と判断し、(3)の場合、コンテンツの配信を禁止する。

(15) 実施の形態2では、無効化情報を受信した宅内サーバ320は、TV420及び520に、認証鍵無効化情報を送信するとしたが、宅内サーバ320は、受け取った無効化情報をTV420及び520に送信するとしても良い。

【0084】

この構成の場合、認証鍵Key24を宅内サーバ320に登録する際、専用端末120から機器識別子ID4、認証鍵Key24及びModule-2を受け取った宅内サーバ320は、Module-2をTV420に送信する。TV420は、受信したModule-2と優先順位が上位の認証鍵とを対応付けて記憶する。TV520も同様の処理を行う。

【0085】

宅内サーバ320は無効化情報を受信すると、受信した無効化情報をTV420及び520に送信する。TV420及びTV520は、優先順位が上位の認証鍵と対応付けて記憶しているModule-2と、受信した無効化情報に含まれる無効化専用端末のIDとが一致するか否かを判断し、一致する場合、Module-2を削除する。また、宅内の全ての機器が、管理装置920から無効化情報を受信し、受信した機器はそれぞれ、認証鍵の無効化を判断するようにしても良い。

(16) 実施の形態2では、TV420及び520は、認証鍵無効化情報を受信すると、認証鍵を削除するとしたが、本発明はこれに限定されない。認証鍵が無効化され、使用できないことを判断できれば良い。

【0086】

例えば、予め認証鍵に無効化フラグを付しておき、認証鍵無効化情報を受信すると、認証鍵無効化情報に含まれる認証鍵と一致する認証鍵に付されている無効化フラグを、無効化に書き換える構成でも良い。

(17) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0087】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものであるとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0088】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0089】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(18) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0090】

【発明の効果】

以上説明したように、本発明は、第1機器と第2機器との間において、認証を行う認証システムであって、前記第2機器に固有の識別子の入力を受け付け、所定の鍵生成アルゴリズムに基づいて前記識別子から第1鍵データを生成し、生成した第1鍵データを前記第1機器に送信する鍵登録装置と、前記鍵登録装置から前記第1鍵データを受信して記憶し、当該第1鍵データを用いて前記第2機器を認証する第1機器と、前記識別子から前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成される第2鍵データを予め記憶しており、前記第2鍵データを用いて前記第1機器による認証を受ける第2機器とから構成されることを特徴とする認証システムである。

【0091】

また、本発明は、第1機器と第2機器との間において、認証を行う認証システムであって、前記第2機器に固有の機器識別子の入力を受け付け、鍵生成アルゴリズムに基づいて前記機器識別子から第1鍵データを生成し、生成した第1鍵データを前記第1機器に送信する鍵登録装置と、前記鍵登録装置から受信する前記第1鍵データを記憶し、前記第1鍵データを用いて前記第2機器を認証する第1機器と、前記機器識別子からそれぞれ異なる鍵生成アルゴリズムに従って生成される複数の鍵データを予め記憶しており、前記複数の鍵データの内の、前記鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第2鍵データを選択し、選択した第2鍵データを用いて、前記第1機器による認証を受ける第2機器とから構成されることを特徴とする認証システムである。

【0092】

また、本発明は、第2機器が有する、第1機器と前記第2機器との間で認証を行うための第2鍵データと同一の第1鍵データを、前記第1機器に設定する鍵登録装置であって、前記第2機器に固有の識別子の入力を受け付ける入力手段と、鍵生成アルゴリズムを有し、前記鍵生成アルゴリズムに基づいて、前記識別子から前記第1鍵データを生成する鍵データ生成手段と、生成した前記第1鍵データを前記第1機器へ出力する出力手段とから構成

されることを特徴とする鍵登録装置である。

【0093】

この構成によると、鍵登録装置を用いない限り、第1機器に第2機器の鍵を登録することは出来ないの、登録された機器以外と通信することを防ぐ。これにより、コンテンツをユーザ宅内での個人使用に限定することが出来る。また、外部への接続手段を持たない機器でも実現できる。

ここで、前記第1機器は、更に、鍵登録装置の無効化を管理する管理機関により生成され、前記鍵登録装置の無効化を示す鍵無効化情報を受け取り、前記鍵登録装置から受信した第1鍵データを無効化し、前記第2機器は、前記鍵無効化情報を受け取り、前記第2鍵データを無効化するようにしても良い。

10

【0094】

この構成によると、無効化された鍵登録装置で登録した鍵データは無効化されるので、不正に鍵登録装置を用いて鍵データが登録されても、無効化することが出来る。

ここで、前記認証システムは、更に、鍵再登録装置を含み、前記鍵再登録装置は、前記第2機器に固有の機器識別子の入力を受け付け、前記鍵登録装置の鍵生成アルゴリズムと異なる鍵生成アルゴリズムに基づいて前記第2機器に固有な機器識別子から第3鍵データを生成し、生成した第3鍵データと前記機器識別子とを前記第1機器に送信し、前記第1機器は、更に、前記鍵再登録装置から受信する前記第3鍵データ及び前記機器識別子を対応付けて記憶し、前記第3鍵データを用いて前記第2機器を認証し、前記第2機器は、更に、前記複数の鍵データの内、前記第3鍵データを生成した鍵生成アルゴリズムと同一の鍵生成アルゴリズムに基づいて生成された第4鍵データを用いて、前記第1機器による認証を受けるようにしても良い。

20

【0095】

この構成によると、登録した鍵データが無効化されても、第2機器は複数の鍵データを持つので、正規の鍵再登録装置を用いることによって、第1機器に新たに鍵データを登録することが出来る。

ここで、前記第1機器は、前記管理機関により生成され、無効化された鍵登録装置に固有の識別子を更に含む鍵無効化情報を受け取り、更に受け取った識別子を無効化識別子として記憶し、鍵登録装置から、第1鍵データと共に、前記鍵登録装置に固有の識別子を受け取り、受け取った識別子が前記無効化識別子と一致するか否かを判断し、一致する場合、前記鍵登録装置から前記第1鍵データを受け取ることを拒否するようにしても良い。

30

【0096】

この構成によると、第1機器は、無効化された鍵登録装置の識別子を無効化識別子として記憶しているの、無効化された鍵登録装置を用いて鍵データを登録しようとしても拒否し、不正に鍵データを登録することを防ぐことが出来る。

ここで、前記第1機器は、前記管理機関により生成され、前記鍵無効化情報に前記管理機関の署名を施して生成された署名データを更に含む前記鍵無効化情報を受け取り、前記署名データを検証し、検証結果が成功であれば、前記識別子を無効化識別子として記憶するようにしても良い。

【0097】

この構成によると、第1機器は、鍵無効化情報に含まれる署名データの検証結果が成功の場合に、無効化識別子として記憶するので、前記管理機関によって発行されたことを確認することが出来、改ざんされているか否かを確認できる。これにより、不正に鍵データを登録されることを防ぐ。

40

ここで、前記出力手段は、前記第1鍵データを暗号化して前記第1機器へ出力し、前記第1機器は、暗号化された第1鍵データを受け取り、復号するようにしても良い。

【0098】

また、前記鍵登録装置は、前記第1機器を認証する認証手段を含み、前記鍵データ生成手段は、前記認証手段による認証結果が成功の場合、前記第1鍵データを生成するようにしても良い。

50

この構成によると、鍵データの不正利用を防止し、正規の機器の鍵データを登録することが出来る。

【0099】

ここで、前記出力手段は、前記第1鍵データを、ネットワークを介して前記第1機器へ送信し、前記第1機器は、ネットワークを介して前記第1鍵データを受信するようにしても良い。

この構成によると、ネットワークを介して鍵データを登録するので、サービスマンが鍵登録装置を持ってユーザ宅内に行かなくても、ネットワークに接続できる任意の場所から鍵データを登録することが出来る。

【図面の簡単な説明】

【図1】認証システム1100の全体の構成を示すブロック図である。

【図2】専用端末100及び宅内サーバ300の構成を示すブロック図である。

【図3】宅内サーバ300及びTV400の構成を示すブロック図である。

【図4】制御部101の動作を示すフローチャートである。

【図5】制御部301が鍵を登録する際の動作を示すフローチャートである。

【図6】制御部301がコンテンツをTV400に配信する際の動作を示すフローチャートである。

【図7】認証部307と認証部402との相互認証の際の動作を示すフローチャートである。

【図8】認証システム1200の全体の構成を示すブロック図である。

【図9】記憶部325の内部の構成を示すブロック図である。

【図10】認証鍵Key14を記憶した際の記憶領域330の内部の構成を示すブロック図である。

【図11】専用端末120が無効化された際の記憶領域330の内部の構成を示すブロック図である。

【図12】専用端末140で再登録した際の記憶領域330の内部の構成を示すブロック図である。

【図13】制御部321の動作を示すフローチャートである。

【図14】認証システム1300の全体の構成を示すブロック図である。

【図15】専用端末120の構成を示すブロック図である。

【図16】専用端末140の構成を示すブロック図である。

【図17】宅内サーバ320の構成を示すブロック図である。

【図18】TV420の構成を示すブロック図である。

【図19】TV520の構成を示すブロック図である。

【符号の説明】

100、120、140 専用端末
 200、220 宅内システム
 300、320 宅内サーバ
 400、420、500、520 TV
 600、620 ルータ
 700 インターネット
 800 コンテンツ配信装置
 900 管理機関
 920 管理装置
 1100 認証システム
 1200 認証システム
 1300 認証システム

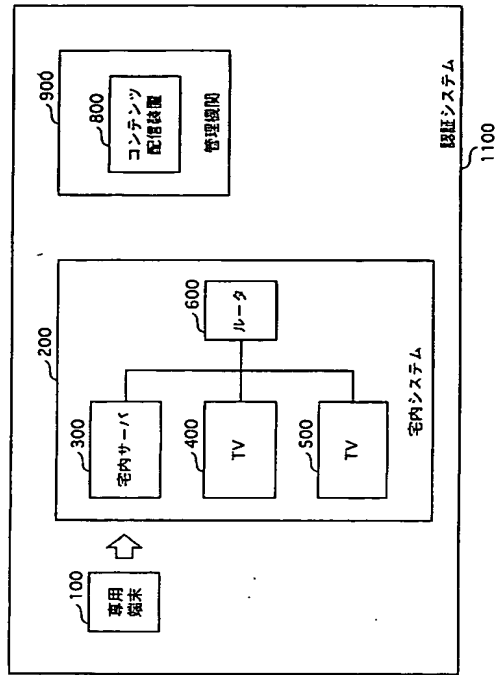
10

20

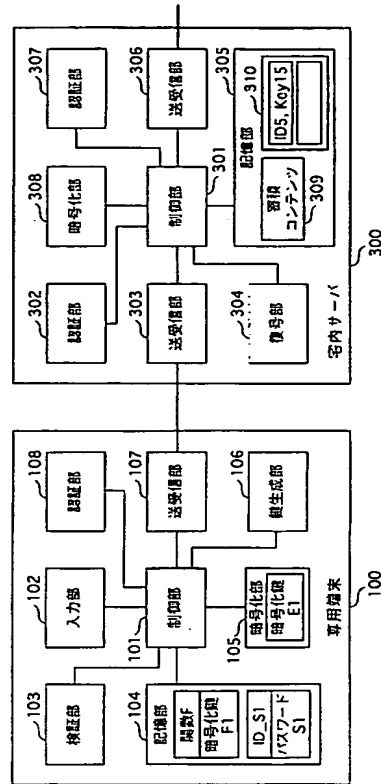
30

40

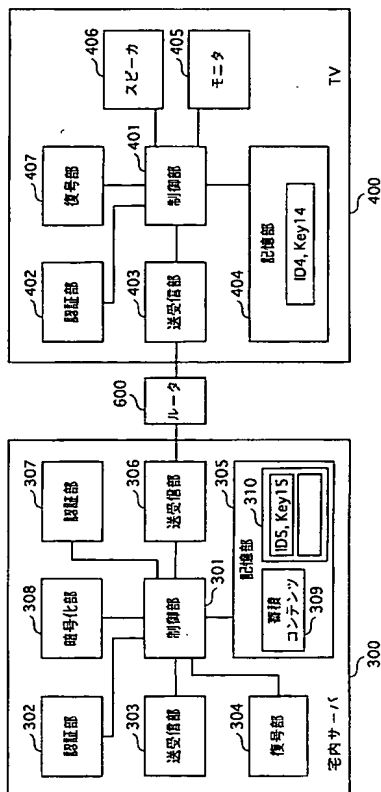
【図 1】



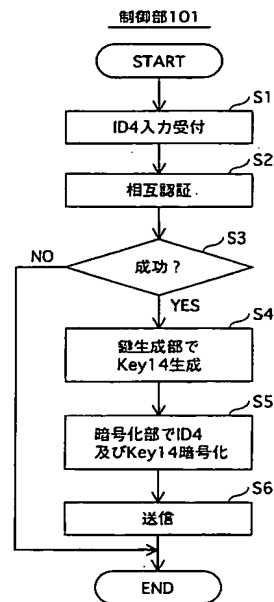
【図 2】



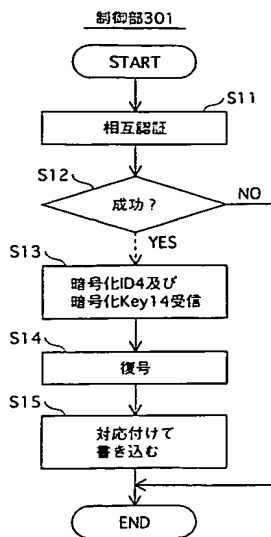
【図 3】



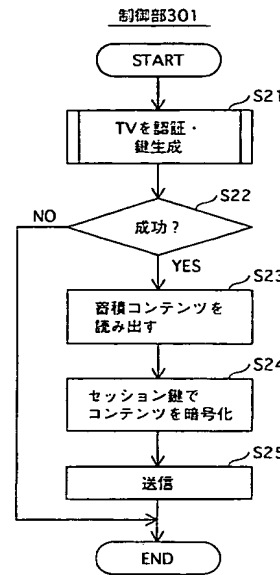
【図 4】



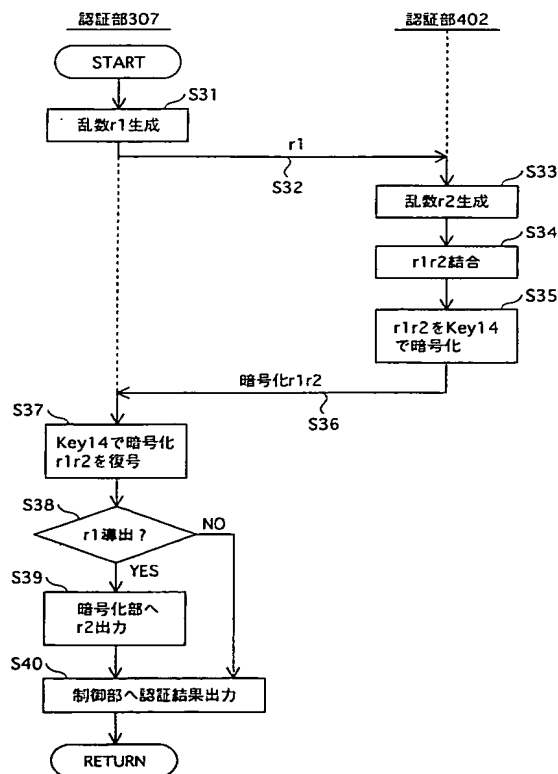
【図 5】



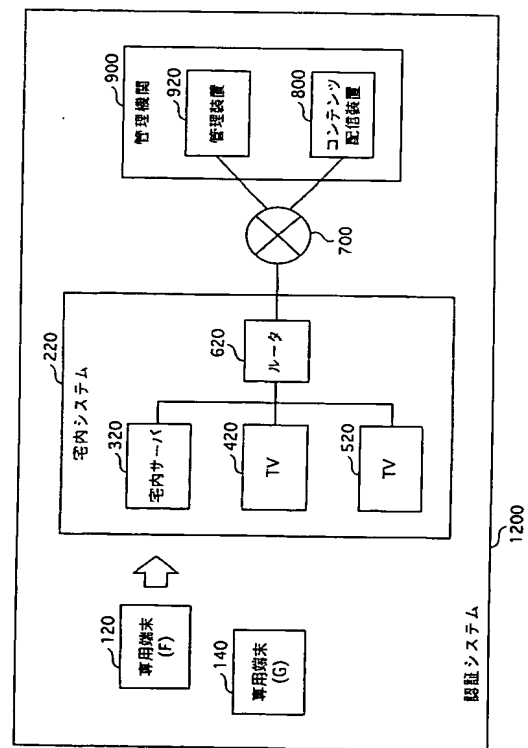
【図 6】



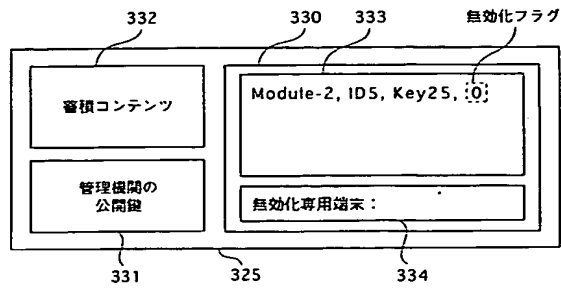
【図 7】



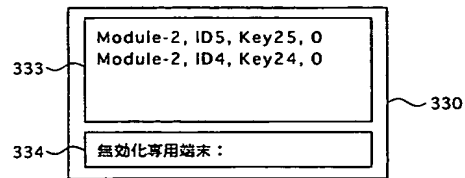
【図 8】



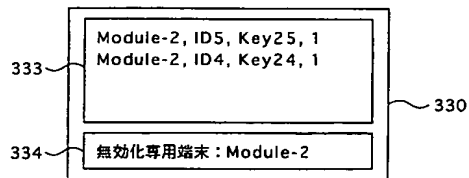
【図 9】



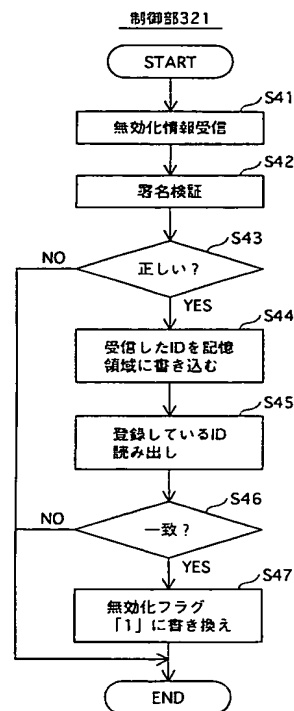
【図 10】



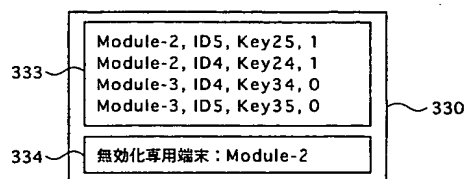
【図 11】



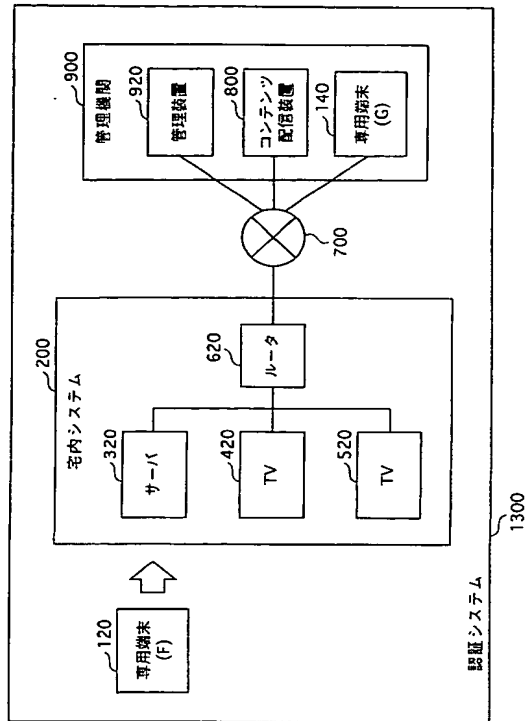
【図 13】



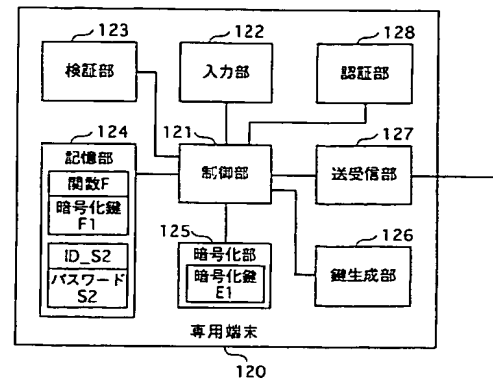
【図 12】



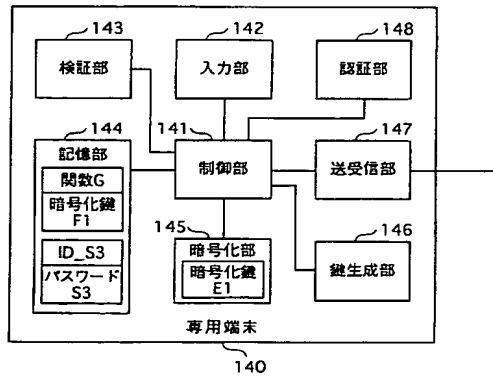
【図 14】



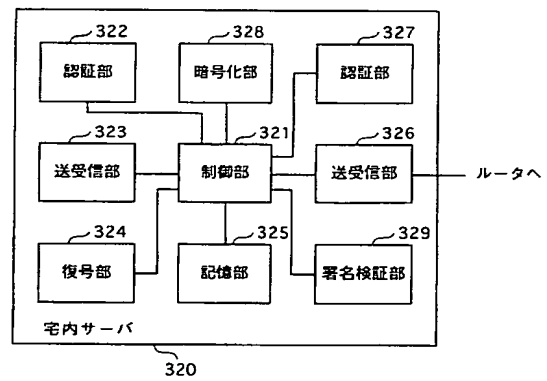
【図 15】



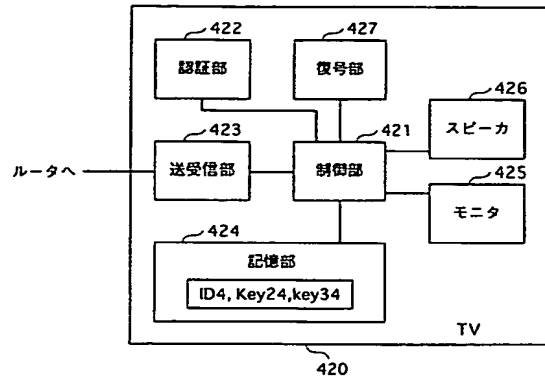
【図 16】



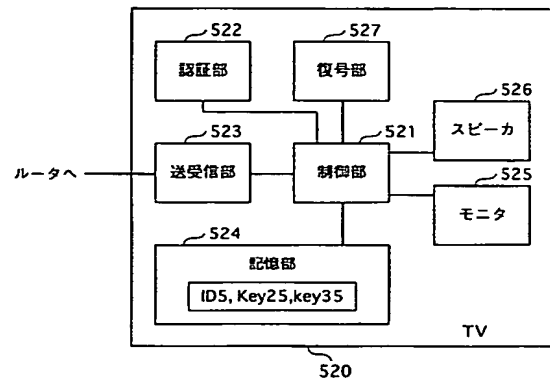
【図 17】



【図 18】



【図 19】



フロントページの続き

(72)発明者 布田 裕一

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72)発明者 大森 基司

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72)発明者 北虎 裕人

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Ｆターム(参考) 5J104 AA07 AA12 AA16 AA34 EA04 EA15 EA16 EA18 JA03 JA21

JA29 KA02 KA04 KA06 KA15 MA05 NA02 NA05 NA27 NA35

NA37